Bilad Alrafidain Journal for Engineering Science and Technology
https://dx.doi.org/10.56990/bajest/2026.050111
ISSN: 2073-9524
Pages:124-134

Federated Learning Based Intelligent Spectrum Management for Secure Cognitive IoT Communications

Nbras Jomah Mohammed Khalaf[1]*
[1] Department of Fundamentals of Religion/Al -Imam Al-Aʿzam University College, Diyala, 32001, Iraq
nibras.juma@imamaladham.edu.iq

Abstract

The increasing density of IoT devices has intensified spectrum scarcity and security challenges in modern wireless communication systems. Conventional spectrum allocation mechanisms are centralized, static, and vulnerable to privacy leakage and malicious attacks. This paper proposes a federated learning–based intelligent spectrum management framework for cognitive IoT networks. Unlike traditional centralized learning, the proposed approach enables distributed IoT nodes to collaboratively train a global spectrum decision model without sharing raw data, thereby preserving privacy and enhancing security. Each node locally learns spectrum availability patterns and interference characteristics, while a lightweight aggregation mechanism updates the global model. Simulation results show that the proposed framework improves spectrum utilization efficiency, reduces interference, and enhances communication security compared to centralized and non-intelligent spectrum management schemes.

Keywords: Federated Learning, Cognitive Radio, IoT Communications, Spectrum Management, Secure Wireless Networks

Article history: **Received:**9 Feb 2026**, Accepted:** 6 March 2026**, Published:** 15 Mar 2026**.**

1. Introduction

The recent fast growth of Internet of Things (IoT) gadgets has essentially changed the contemporary wireless communication systems so that they can be used in large numbers to provide connectivity to different applications like smart cities [1], industrial automation, health care monitoring, and smart transportation. Nevertheless, this huge usage of heterogeneous and resource-constrained devices has resulted in serious instances of spectrum scarcity, interference, and security of communication. The inflexible and fixed spectrum allocation policy historically followed in wireless networking can no longer offer the dynamic and dense characteristics of cognitive IoT settings [1], [2], and [3].

Cognitive radio (CR) technology has been proposed as a solution to spectrum scarcity to enable IoT devices to opportunistically access underutilized frequencies. Cognitive IoT networks can also contribute to high-efficiency spectrum utilization by sensing the radio environment and controlling the transmission parameters on it [4] and [5]. However, spectrum management in such networks involves efficient spectrum availability learning, interference structure, and user Behaviour, which grows progressively more complex with the scale and dynamics of networks. In the recent past, spectrum management methods employing machine learning (ML) have received significant research attention in order to facilitate intelligent decision-making in cognitive radio networks. These can be trained over intricate patterns in the environment and maximize spectrum access plans. Nevertheless, the majority of current ML-related solutions are built upon centralized learning systems, where raw sensing

* Corresponding author: nibras.juma@imamaladham.edu.iq

information of distributed IoT nodes is gathered at a central server to train a model. This centralized paradigm has several serious limitations, such as the high communication overhead, scalability, one-point failure, and severe privacy and security threats, particularly when sensitive spectrum usage information is being disclosed [6] and[9].

Federated learning (FL) is a recently emerging privacy-safe distributed learning paradigm that provides the ability to train models collaboratively without having to transmit raw local data. Each IoT node does the local model training instead of sending sensitive observations to a central entity, and only sends model updates to an aggregation server. With this decentralized learning approach, the privacy leakage is inherently minimized, and the attack surfaces are minimized, which is suitable in the distributed nature of cognitive IoT networks as well. Notwithstanding the opportunities, little is known about the application of federated learning to intelligent spectrum management to secure cognitive IoT communications [10] and [12].

These observations are the driving factor for why a federated learning-based intelligent spectrum management framework has been suggested in this paper to manage cognitive IoT networks. The solution suggested allows distributed IoT nodes to learn the spectrum access policies together, maintain data privacy, and increase the security of communications. The local sensing of spectral availability and the interference properties of each node is implemented, and a small-scale federated aggregation scheme is adopted to build a strong global decision model. By thoroughly simulating the proposed framework, it is demonstrated to be more efficient in spectrum utilization, with less interference, and offers better security than centralized learning and other traditional non-intelligent spectrum management schemes.

The rest of this paper will be structured in the following way: Section II will provide a review of related literature on intelligent spectrum management and federation learning in wireless networks. Section III introduces the suggested federated learning-based spectrum management. Section IV presents the performance evaluation and the simulation setup. Section V presents the findings, and Section VI is the conclusion of the paper in terms of future research directions.

2. Related Works

The recent study of intelligent spectrum management in cognitive IoT networks has paid more attention to utilizing machine learning (ML) and distributed intelligence to overcome the problem of spectrum scarcity, interference, and security issues. Spectrum sensing and decision-making methods based on deep learning have proven to be more effective than the standard energy detection methods because they can detect the multifaceted time-frequency correlations of dynamic radio conditions. Nevertheless, many of these methods are based on centralized architectures of learning, where raw sensing data are sent to a fusion center or cloud server to train a model. The problem with such centralized designs is that they have high communication overhead, limited scalability, and are prone to single-point failures coupled with leakage of privacy information, thus making them unsuitable for the large-scale implementation of IoT with privacy sensitivities.

Federated learning (FL) has proven to be an effective solution to these shortcomings as a potential paradigm of cooperative spectrum sensing and spectrum occupancy detection. Wasilewska et al. [13] proposed an FL-based spectrum sensing framework of 5G systems and showed that joint model training is possible without moving sensing information to remote locations, hence ensuring privacy. Kopacz et al. [14] also extended FL to distributed spectrum occupancy detection, with a higher detection accuracy achieved in the case of heterogeneous data distributions. More recently, it has also considered decentralized and serverless FL architecture to minimize the use of central aggregators; e.g., Cata et al. [15] examined serverless FL in the context of cooperative spectrum sensing in non-IID conditions and demonstrated improved robustness and scalability. Although these studies can prove the applicability of FL in collaborative sensing, they largely concentrate on binary occupancy detection and not on the entire spectrum management process.

In addition to sensing, the technique of federated learning has been used in spectrum sharing problems and dynamic spectrum access (DSA). According to Song et al. [16] suggested federated DSA framework has the potential to learn spectrum access strategies without centralizing the terminal data, which is the key feature of FL to adapt to the heterogeneous network conditions. The work of Dong et al. [17] built on federated learning through spectrum access to add federated and online reinforcement learning to dynamic spectrum access to wireless networks, which facilitates autonomous choice of channels with lower coordination cost.

In addition to dynamic spectrum access, federated learning-based radio resource management and spectrum allocation schemes have been explored to support beyond-5G and 6G networks and have shown that distributed learning can be successfully deployed to support spectrum sharing across a wide variety of traffic and interference scenarios. Federated deep reinforcement learning methods have also been studied more recently in the case of IoT-oriented dynamic spectrum access applications and application-specific spectrum sharing, such as smart grid and emergency radio systems.

In spite of these developments, security and robustness are serious issues of concern. FL does not necessarily result in the exchange of raw data, though it brings about other threats of model poisoning, Byzantine attacks, and inference attacks on shared updates. Safe aggregation schemes and adversary-biased learning algorithms play an essential role and are extensively studied [18] and [19]. When using open and decentralized wireless systems. Wasilewska et al. [20], in the context of the cognitive radio, pointed out the problem of reliability and security peculiar to FL-based spectrum sensing and elaborated on measures to prevent malicious players.

The current research on FL-enabled cognitive radio and IoT networks mainly focuses on cooperative sensing or more limited dynamic spectrum access issues. There are relatively fewer papers that cover end-to-end intelligent spectrum management that considers jointly spectrum availability learning, access decisions made based on interference, and clear security and privacy goals when non-IID data distributions are realistic. It is this gap that drives the creation of an intelligent spectrum management framework using federated learning and designed to support secure cognitive IoT communications, as suggested in this work.

3. Problem Formulation and System Model

3.1. System Model

We assume a cognitive IoT network that comprises a group of distributed IoT devices $\mathcal{N} = \{1,2,\dots,N\}$ operating in a shared wireless environment with a finite set of licensed and unlicensed spectrum channels $\mathcal{C} = \{1,2,\dots,C\}$

The cognitive radio capabilities in each IoT node enable it to monitor spectrum occupancy, estimate interference levels, and opportunistically use available channels without causing detrimental interference to primary users (PUs) or other IoT devices. Time is divided into discrete slots $t \in \{1,2,\dots,T\}$ At each time slot, each node performs local spectrum sensing and observes a feature vector [26].

$$\mathbf{x}_i(t) = [o_i^1(t), o_i^2(t), \dots, o_i^C(t), I_i(t)] \quad (1)$$

Where $o_i^c(t) \in \{0,1\}$denotes the occupancy state of channel $c$as perceived by node i, and $I_i(t)$represents the measured interference or signal-to-interference-plus-noise ratio ($\mathrm{S}c_i(t) \in \mathcal{C}$for transmission.

The collaborative learning is supported by a federated learning server (aggregator). Raw sensing data is not shared with the server, but it incorporates local model changes based on the involvement of the IoT nodes in constructing a global spectrum decision model.

3.2. Federated Learning-Based Spectrum Decision Model

Each IoT node maintains a local model parameterized by bi, which MI. Local observations $\mathbf{x}_i(t)$to a spectrum access decision. The local learning objective of node $i$is defined as:

$$\min_{\boldsymbol{\theta}_i} \ \mathcal{L}_i(\boldsymbol{\theta}_i), \quad (2)$$

Here $\mathcal{L}_i(\cdot)$is a local loss function capturing spectrum access performance, such as collision probability, interference level, or reward-based access success. Under the federated learning

paradigm, the global optimization problem is formulated as [27]:

$$\min_{\boldsymbol{\theta}} \quad \sum_{i=1}^{N} \frac{|\mathcal{D}_i|}{\sum_{j=1}^{N}|\mathcal{D}_j|}\mathcal{L}_i(\boldsymbol{\theta}) \qquad (3)$$

Where $\mathcal{D}_i$denotes the local dataset of node i, and $\boldsymbol{\theta}$represents the global model parameters. At each communication round, nodes locally update their models using stochastic gradient descent and transmit only the updated parameters. $\boldsymbol{\theta}_i$to the server. The server performs federated averaging (FedAvg) to obtain the global model [27]:

$$w_i = \frac{|\mathcal{D}_i|}{\sum_{j=1}^{N}|\mathcal{D}_j|}, \boldsymbol{\theta}^{(t+1)} = \sum_{i=1}^{N} w_i \boldsymbol{\theta}_i^{(t)} \qquad (4)$$

The updated global model is then broadcast back to all nodes for the next learning round.

3.3. Problem Formulation

The proposed federated learning-based framework has the aim of attaining smart, safe, and effective spectrum management regarding cognitive IoT networks. In particular, the spectrum decision problem is established to optimize spectrum utilization, minimize interference, improve the quality of communication, and maintain data privacy. The spectrum utilization, collision, SINR, and throughput models are based on conventional models that are common in the literature on cognitive radio and wireless communication [21-24], and the joint optimization based on federated learning is inspired by current developments in distributed wireless intelligence [25].

A) Spectrum Utilization Efficiency

The spectrum utilization efficiency is defined as the ratio of successfully accessed idle channels to the total available spectrum resources over the observation period. It is formulated as [28]:

$$\max \; U = \frac{\sum_{t=1}^{T}\sum_{i=1}^{N}\mathbb{1}\,(c_i(t) \text{ is idle})}{T \cdot C}, \qquad (5)$$

Where $\mathbb{1}(\cdot)$is an indicator function that equals 1 if i. selective electei$c_i(t)$is idle at time slot t, and 0 otherwise. Maximizing Uensures efficient exploitation of available spectrum opportunities and minimizes idle spectrum wastage.

B) Collision and Interference Minimization

To minimize the destructive interference and collisions between the IoT devices, the probability of collision is minimized by punishing multiple nodes that simultaneously select a channel. This goal is formulated as [29].

$$\mathcal{C} = \sum_{t=1}^{T}\sum_{i\neq j}\mathbb{1}\left(c_i(t) = c_j(t)\right), \qquad (6)$$

Where a is the number of collisions in the IoT, which is considered the selection of a channel by two or more nodes at the same time slot. Reducing this goal results in interference-linked spectrum access choices, which are vital in large-scale IoT applications.

C) Communication Quality: SINR Maximization

The communication quality of each IoT node is evaluated using the signal-to-interference-plus-noise ratio (SINR). For node $i$at time slot t, the SINR is given by [30]:

$$\text{SINR}_i(t) = \frac{P_i(t)g_{ii}(t)}{\sigma^2 + \sum_{j\neq i}P_j(t)g_{ji}(t)} \qquad (7)$$

i.e., $P_i(t)$is the transmission power of node i., $g_{ii}(t)$is the channel gain between the transmitter and receiver of node i, $g_{ji}(t)$represents the interference channel gain from node j, and σ^2denotes the noise power. Maximizing SINR improves link reliability and communication robustness.

D) Throughput Maximization

Using the Shannon capacity formula, the achievable throughput of node i was given by the following, depending on the achieved SINR of node i.

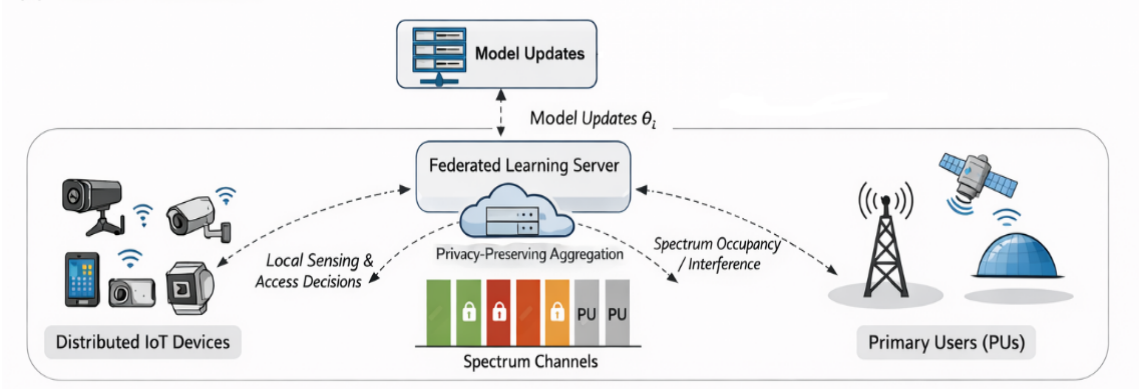
$$R_i(t) = B\log 2_2\left(1 + \text{SINR}_i(t)\right), \qquad (8)$$

where $B$is the channel bandwidth. The average network throughput is obtained by averaging. $R_i(t)$over all IoT nodes and time slots. Maximizing throughput ensures efficient data transmission and improved quality of service.

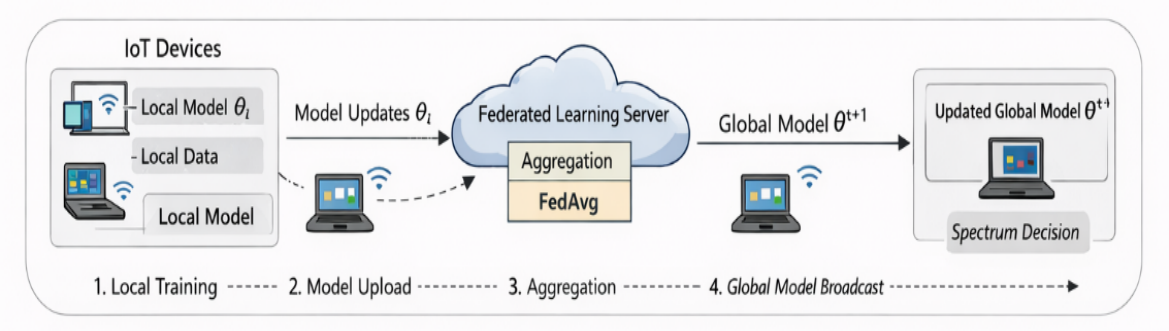
These goals are to be achieved within feasible limitations, such as the limited computational and energy capacity of the IoT devices, non-IID local data distributions, dynamic spectrum accessibility, and a possible malicious or unreliable set of participants. Fig.1 shows the general scheme of the proposed federated cognitive IoT network, comprising both

ISSN: 2073-9524
Pages:124-134

network architecture and the federated learning workflow of intelligent and privacy-preserving spectrum management [31].



(A) Network architecture with distributed IoT devices and a federated learning server under primary user constraints.



(B) Federated learning workflow for privacy-preserving intelligent spectrum management.

Fig. 1 System model of the proposed federated learning–based cognitive IoT network.

4. Proposed Federated Learning–Based Intelligent Spectrum Management Method

This section presents the proposed federated learning (FL)–based intelligent spectrum management method for secure cognitive IoT communications. The objective of the proposed method is to enable distributed IoT nodes to perform efficient and secure spectrum access decisions while preserving data privacy and reducing the vulnerabilities associated with centralized spectrum management.

4.1. Overall Framework Overview

As illustrated in Fig. 1 and Fig. 2, the proposed framework consists of three main components:

1. Local spectrum sensing and learning at IoT nodes,
2. Federated aggregation at a central server, and
3. Global model dissemination for cooperative spectrum decision-making.

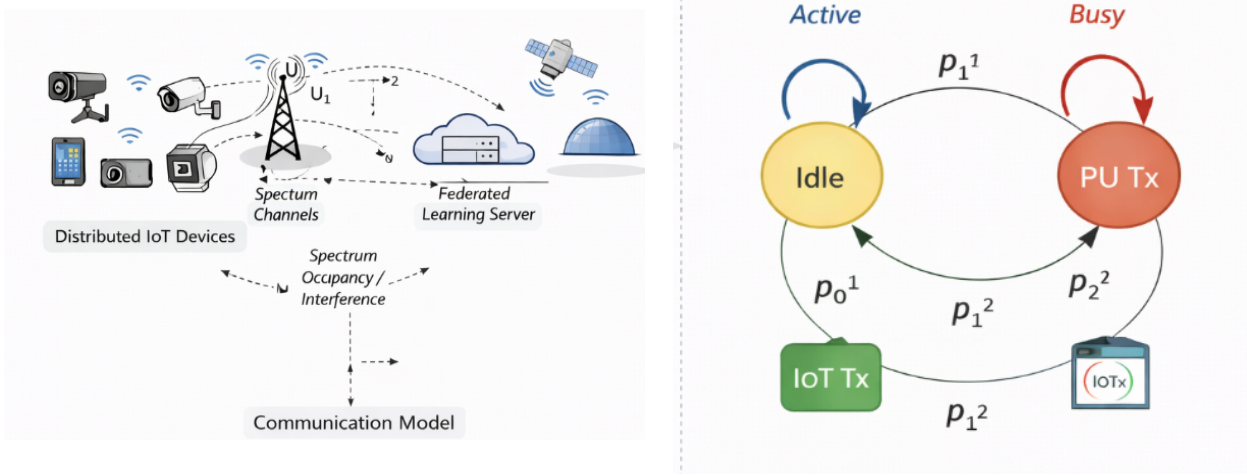
Each IoT node operates autonomously by sensing the radio environment and learning local spectrum usage patterns. Instead of transmitting raw sensing data to a centralized controller, nodes participate in a federated learning process where only model updates are exchanged. This design significantly reduces communication overhead, preserves data privacy, and improves robustness against malicious attacks.

4.2. Local Spectrum Sensing and Feature Extraction

At each time slot t, each IoT node $i$performs spectrum sensing over the available channels and constructs a local observation vector as defined in Eq. (1). The extracted features include channel occupancy indicators, interference measurements, and signal quality indicators such as the signal-to-interference-plus-noise ratio (SINR). These features capture both temporal and spatial variations of spectrum availability. Due to heterogeneous deployment environments and varying proximity to primary users and neighboring IoT devices, the collected local datasets are inherently non-IID,

ISSN: 2073-9524
Pages:124-134

reflecting realistic cognitive IoT network conditions. The communication and state-transition behavior of spectrum usage is modeled using the communication model and state diagram shown in Fig. 2 [27].



(A) Communication model in cognitive

(B) State diagram representing the Markov chain for spectrum decision-making.

Fig. 2 Communication model and state diagram for spectrum decision.

4.3. Local Model Training at IoT Nodes

Each IoT node maintains a lightweight local learning model parameterized by$\boldsymbol{\theta_i}$. The model learns a mapping from the local observation vector to a spectrum access decision or channel selection probability. The local training objective is to minimize a loss function that penalizes collisions, interference, and unsuccessful transmissions, as formulated in Eq. (2). Local model updates are performed using stochastic gradient descent (SGD) or Adam optimization over a limited number of local epochs to ensure computational efficiency and energy awareness, which are critical requirements for resource-constrained IoT devices.

4.4. Federated Aggregation and Global Model Update

After completing local training, participating IoT nodes transmit only their updated model parameters. $\boldsymbol{\theta_i}$to the federated learning server. No raw sensing data or local observations are shared. The server aggregates the received parameters using the FedAvg strategy defined in Eq. (3) to compute an updated global model. This aggregation process is repeated over multiple communication rounds. The convergence behavior of the global model is evaluated and illustrated in Fig. 3, demonstrating stable learning performance despite non-IID data distributions and partial device participation. This comparison highlights the convergence characteristics of the proposed learning process rather than its final performance.

4.5. Global Model Dissemination and Spectrum Decision

The unified worldwide design is transmitted to all the IoT nodes. Each node then uses the revised global model to make its decisions on channel selections in later time slots. Such a cooperative learning process allows nodes to take advantage of common knowledge about the spectrum environment and retain full control over their local data. The decisions to be reached on the spectrum are aimed at:

- Maximize the efficiency of spectrum utilization (Eq. (4), which is assessed in Fig. 4),
- Reduce the probability of collision and interference (Eq. (5), which is assessed in Fig. 5) and
- Improve the level of communication (SINR) and throughput (Eq. 6) and (Eq. 7), evaluated in Fig. 6.

ISSN: 2073-9524
Pages:124-134

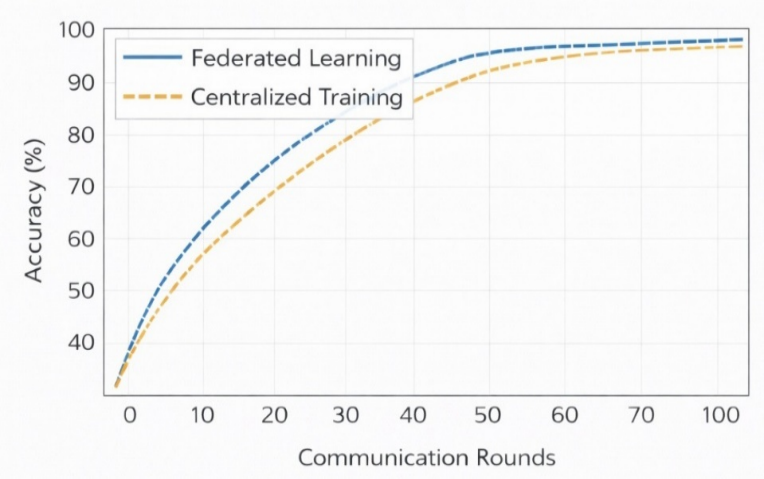


Fig. 3 Convergence behavior of the global model in terms of accuracy versus communication rounds, comparing federated learning with centralized training.

4.6. Security and Privacy Advantages

The proposed method inherently enhances security and privacy by design. Since raw sensing data never leaves local devices, the risk of data leakage and eavesdropping is significantly reduced. Moreover, the distributed learning paradigm mitigates single-point failures commonly observed in centralized spectrum management systems.

5. Simulation Results and Discussion

This part analyzes how the intelligent spectrum management framework in the form of federated learning is performing under ample simulated conditions. The proposed solution is contrasted with a centralized learning-based scheme to establish its usefulness on convergent behavior, spectrum usage efficiency, probability of collisions, and communication quality. To stabilize and be fair, all the results that are reported are averaged across a series of simulation runs.

5.1. Convergence Analysis

In Fig. 3, the convergence behavior of the global model is displayed with respect to accuracy versus communication rounds. The proposed federated learning plan exhibits steady and uniform convergence when non-IID local data distribution and biased participation of devices exist. Surprisingly, even though the convergence of the centralized training is marginally higher in the first rounds because of the direct access to the aggregated information, the model of federated learning becomes not inferior to a similar level of accuracy as the training is continued. This finding supports the fact that the suggested federated aggregation approach can successfully learn an effective global model without exchanging uncooked sensing data, confirming that it is appropriate to use it in distributed cognitive IoT systems. The efficiency of spectrum utilization.

5.2. Spectrum Utilization Efficiency

Fig. 4 demonstrates the performance of the proposed framework regarding the spectrum utilization, where the efficiency of spectrum utilization is calculated as indicated in the formula in the following equation (4). The federated learning method shows a much better spectral utilization when compared to centralized training.

This is because it has been enhanced by the cooperative learning mechanism, which allows the IoT nodes to make more informative decisions during spectrum access by exploiting the common world information and knowledge, and adjusting to the local circumstances. Consequently, spectrum idleness is better utilized, thereby resulting in better total spectrum efficiency.

ISSN: 2073-9524
Pages:124-134

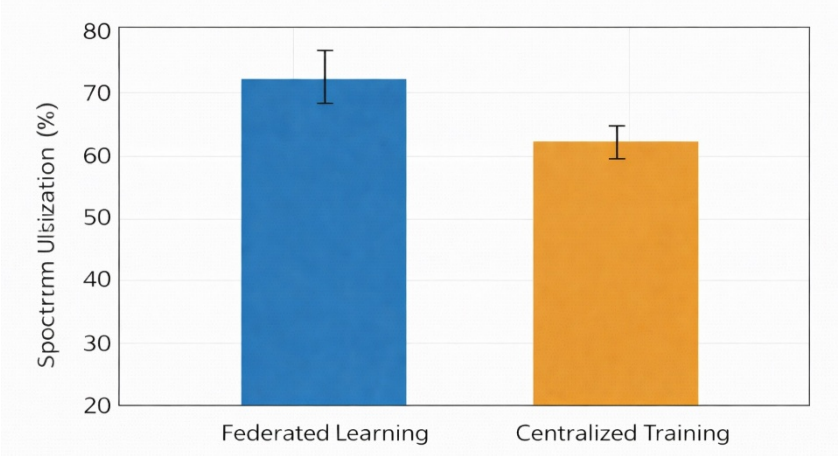


Fig. 4 Spectrum utilization efficiency comparison of the proposed federated learning–based spectrum management framework and the centralized learning scheme under varying network conditions.

5.3. Collision and Interference Analysis

As shown in Fig. 5, the probability of collision of the suggested scheme is compared to the centralized scheme, which is defined in the equation below. The findings indicate that the federated learning approach minimizes the likelihood of collusions and co-channel interference significantly. The proposed framework allows the IoT nodes to better avoid the congested channels by learning the policies of interference-aware spectrum access through distributed observations. This collision reduction is especially significant to dense IoT deployments, where the random access is a highly debilitating network behavior.

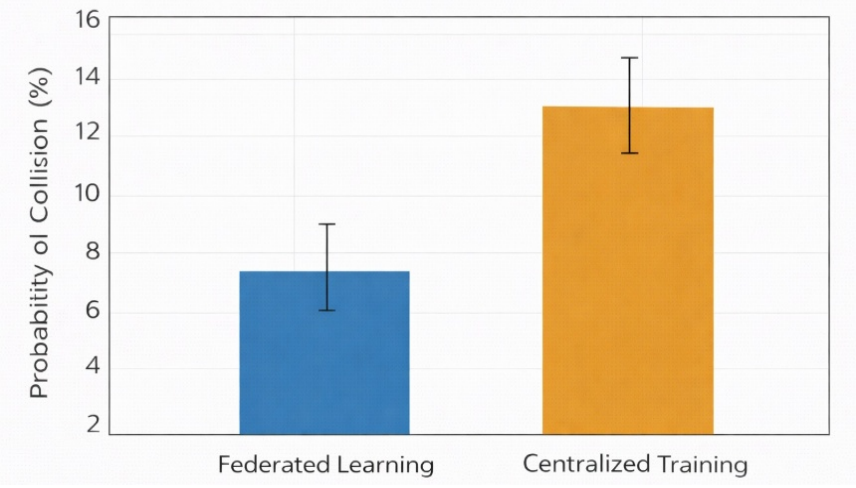
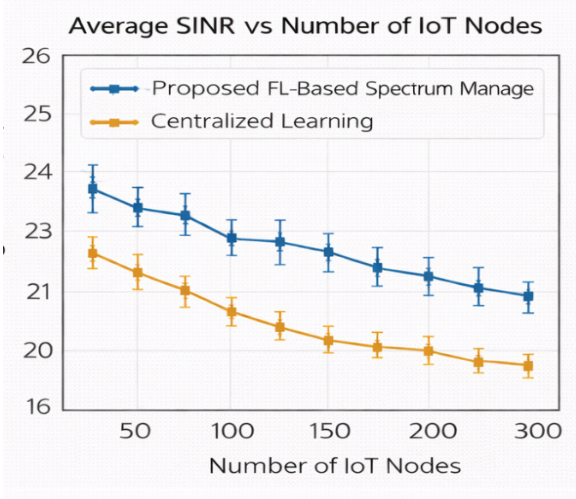


Fig. 5 Collision probability comparison between the proposed federated learning–based spectrum management framework and the centralized learning scheme.

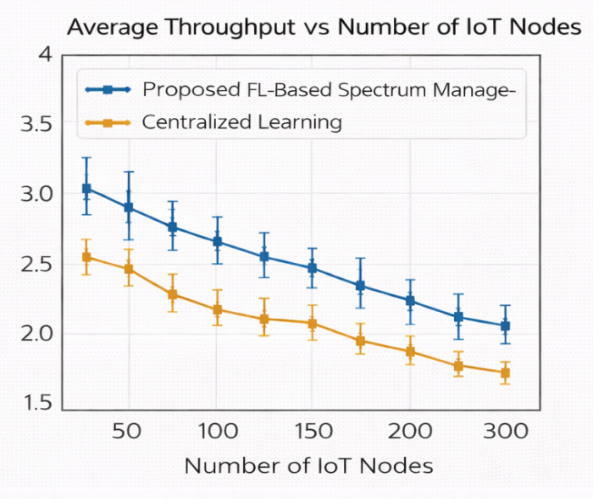
5.4. Quality of Communication: SINR and Throughput.

The communication quality performance is assessed considering average SINR and throughput, which are developed in the form of equations as seen in Fig. (6) and Eq. (7), respectively. As illustrated in Fig. 6, the spectrum management framework proposed using federated learning attains a better SINR and throughput than the centralized one. The enhanced SINR is due to the less interference, and the channel selection is more stable and directly translates to the enhanced data rates. These results show that the suggested method not only enhances spectrum efficiency but end-to-end communication performance as well.

ISSN: 2073-9524
Pages:124-134



(A) Average SINR versus number of IoT nodes.



(B) Average throughput versus number of IoT nodes.

Fig. 6 Communication quality performance comparison

6. Discussion

Overall, the findings of the simulation indicate that the proposed federated learning-based intelligent spectrum management system can achieve a reasonable trade-off among learning performance, spectrum efficiency, and privacy protection in cognitive IoT settings. The proposed scheme is based on the distributive learning of IoT nodes in contrast to centralized learning schemes that use the collection of raw sensing data at the central node, and still allows learning federation. The outcome of this architectural selection is the presence of performance benefits as observed in realistic non-IID data distributions and dynamic spectrum scenarios.

Despite faster convergence as seen in centralized learning in the initial training rounds because of complete information, this reduces as the training advances. The federated learning structure reaches similar convergence Behaviour, as illustrated in Fig. 3, that is, the absence of raw data disclosure does not imply that the global model cannot learn useful spectrum access policies. Such an outcome is of great relevance, especially to cognitive IoT networks, where data heterogeneity and intermittent connectivity are the norm and centralized training is frequently infeasible.

The enhancement of the efficiency of the utilization and the reduction of collisions, shown in Figs. 4 and 5, are explained by the cooperative character of the given process of learning. The global model can capture a wide range of spectrum usage patterns and interference patterns that cannot be perceived by individual nodes or fixed allocation schemes by aggregating distributed knowledge across many nodes of an IoT. As a result, idle opportunities in the spectrum can be exploited better by IoT devices without utilizing congested channels, and the decisions regarding spectrum access are more stable and reliable.

Moreover, the direct effect of smart spectrum control on the quality of communication is demonstrated by the observed improvements in the SINR and throughput (Fig. 6). Lower interference and knowledgeable selection of channels enhance the signal conditions at the receiver and result in increased data rates and greater links. The improvements are particularly useful in high-density IoT networks where uncontrolled access to the spectrum can be disastrous to the network performance and quality of service.

On a system-level, the suggested framework has significant scalability and security benefits. The federated learning paradigm automatically decreases the communication overhead since it sends small updates to the model rather than the sensing data, thus it is appropriate in large-scale IoT networks with limited bandwidth and energy resources. Moreover, with its non-centralized approach to data collection, the framework greatly mediates privacy leakage threats and a single point of failure, which are major issues of concern in security-sensitive cognitive radio applications.

On the whole, the results discussion shows that the suggested federated learning-based spectrum management architecture is not just efficient in enhancing the main performance parameters but also concomitant with the real-world limitations of the cognitive IoT system. Distributed intelligence, preservation of privacy, and adaptive spectrum decision-making make the proposed solution potentially successful as a solution to next-generation secure and scalable cognitive IoT communications.

7. Conclusion

This paper introduced a smart spectrum management system through federated learning of secure cognitive internet of things communications. The suggested approach allows distributed IoT devices to learn to use the devices most effectively in accessing the spectrum without sharing raw sensing information, thus preserving the privacy of the devices and decreasing the susceptibility of centralized spectrum management. The framework, including the use of local spectrum sensing, enables adaptive and interference-aware spectrum decision-making of dynamic and heterogeneous Internet-of-Things settings. A wide range of simulations showed that the convergence of the algorithm was stable when using non-IID data distributions and had better spectral efficiency, lower collision and interference rates, and higher communication quality in terms of SINR and throughput than centralized learning-based algorithms. These findings support the idea that federated learning can be effectively used to balance performance in learning, scalability, and privacy protection in cognitive IoT networks.

8. Future Work

Several directions of research are still available to be explored. To begin with, the framework can be enhanced in terms of strength through the use of safe aggregation in order to address model poisoning and Byzantine attacks. Second, it would be possible to apply the given approach to federated reinforcement learning to make decisions on the adaptive and online spectrum access in a high-dynamics environment. Third, there should be practical implementation issues like reduction of communication overheads, energy-conscious learning, and testbed validation, which should be explored. Lastly, the transfer of the suggested framework beyond 5 G and 6G ultra-dense IoT networks is a research prospect.

Conflict of Interest

The author(s) indicate that there are no known financial or personal associations with persons that may have come out to affect the work being reported in this paper. The research was conducted independently, and the results presented reflect only the scientific findings of the authors.

Acknowledgment:

The authors would like to express their sincere appreciation to the Al -Imam Al-Aʿzam University College for their continuous support and for providing the facilities necessary to carry out this research.

References

[1]. Flores-Iwasaki, M., Guadalupe, G.A., Pachas-Caycho, M., Chapa-Gonza, S., Mori-Zabarburú, R.C., & Guerrero-Abad, J.C. (2025). Internet of Things (IoT) sensors for water quality monitoring in aquaculture systems: A systematic review and bibliometric analysis. Agri Engineering. 7: 78.

[2]. Bandara, R.M.P.N.S., Jayasignhe, A.B., & Retscher, G. (2025). The integration of IoT sensors and location-based services for water quality monitoring: A systematic literature review. *Sensors*. 25: 1918.

[3]. Abdul-Qawy, A.S., Pramod, P., Magesh, E., & Srinivasulu, T. (2015). The Internet of Things (IoT): An overview. *Int. J. Eng. Res. Appl.* 5(12): 71–82.

[4]. Badoi, C.-I., Prasad, N., Croitoru, V., & Prasad, R. (2011). 5G based on cognitive radio. *Wireless. Pers. Commun.* 57(3): 441–464.

[5]. Zheng, R., Li, X., & Chen, Y. (2023). An overview of cognitive radio technology and its applications in civil aviation. *Sensors*. 23: 6125.

[6]. Wang, D., Song, B., Chen, D., & Du, X. (2019). Intelligent cognitive radio in 5G: AI-based hierarchical cognitive cellular networks. *IEEE Wireless. Commun.* 26(3): 54–61.

[7]. Violos, J., Mamanis, G., Kompatsiaris, I., & Papadopoulos, S. (2025). Cognition and context-aware decision-making systems for a sustainable planet: A survey. *Discover Sustain.* 6(1): 1–43.

[8]. Giral, D., Hernández, C., & Rodríguez-Colina, E. (2020). Spectrum decision-making in collaborative cognitive radio networks. *Appl. Sci.* 10(19): 6786.

[9]. Wang, H., Han, X., Cai, B., Liao, G., & Quan, Y. (2025). A unified anti-jamming design in complex environments based on cross-modal fusion and intelligent decision-making. *arXiv preprint*. arXiv:2506.07532.

[10]. Mavire, S., Muhwati, K.B., Kudaro, C.D., & Awoleye, J. (2025). A federated learning approach to secure AI-based patient outcome prediction across hospitals. *Int. J. Sci. Manag. Res.* 8(2): 52–72.

[11]. Kamatala, S. (2025). Federated learning with transformers: Privacy-preserving AI at scale. *Int. J. Comput. Tech.* 12(1): 1–10.

[12]. Akinsiku, A.M. (2025). Federated learning techniques for privacy-preserving AI in distributed networks: A review. *Tech-Sphere J. Pure Appl. Sci.* 2(1): 69–83.

[13]. Wasilewska, M., Bogucka, H., & Kliks, A. (2021). Federated learning for 5G radio spectrum sensing. *Sensors*. 22(1): 198.

[14]. Kułacz, Ł., & Kliks, A. (2023). Federated learning-based spectrum occupancy detection. *Sensors*. 23(14): 6436.

[15]. Catak, F.O., Kuzlu, M., Dalveren, Y., & Ozdemir, G. (2025). Serverless federated learning: Decentralized spectrum sensing in heterogeneous networks. *Phys. Commun.* 70: 102634.

[16]. Song, Y., Chang, H.-H., Zhou, Z., Jere, S., & Liu, L. (2021). Federated dynamic spectrum access. *arXiv preprint*. arXiv:2106.14976.

[17]. Dong, X., You, Z., Liu, X., Guo, Y., Shen, Y., & Gong, Y. (2023). Federated and online dynamic spectrum access for mobile secondary users. *IEEE Trans. Wireless. Commun.* 23(2): 621–636.

[18]. Tian, Z., Cui, L., Liang, J., & Yu, S. (2022). A comprehensive survey on poisoning attacks and countermeasures in machine learning. *ACM Comput. Surv.* 55(2): 1–35.

[19]. Manzoor, H.U., Shabbir, A., Chen, A., Flynn, D., & Zoha, A. (2024). A survey of security strategies in federated learning: Defending models, data, and privacy. *Future Internet*. 16(9): 374.

[20]. Wasilewska, M., Bogucka, H., & Poor, H.V. (2023). Secure federated learning for cognitive radio sensing. *IEEE Commun. Mag.* 61(6): 68–73.

[21]. Akyildiz, I.F., Lee, W.-Y., Vuran, M.C., & Mohanty, S. (2006). Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Comput. Netw.* 50(13): 2127–2159.

[22]. Zhao, Q., & Sadler, B.M. (2007). A survey of dynamic spectrum access. *IEEE Signal Process. Mag.* 24(3): 79–89.

[23]. Goldsmith, A. (2005). *Wireless communications*. Cambridge: Cambridge University Press.

[24]. Shannon, C.E. (1948). A mathematical theory of communication. *Bell Syst. Tech. J.* 27(3): 379–423.

[25]. Park, J., Samarakoon, S., Bennis, M., & Debbah, M. (2019). Wireless network intelligence at the edge. *Proc. IEEE*. 107(11): 2204–2239.

[26]. Yucek, T., & Arslan, H. (2009). A survey of spectrum sensing algorithms for cognitive radio applications. IEEE communications surveys & tutorials, 11(1), 116-130.

[27]. McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial Intelligence and statistics (pp. 1273-1282).

[28]. Zhao, Q., & Sadler, B. M. (2007). A survey of dynamic spectrum access. *IEEE signal processing magazine*, *24*(3), 79-89.

[29]. Arjoune, Y., & Kaabouch, N. (2019). A comprehensive survey on spectrum sensing in cognitive radio networks: Recent advances, new challenges, and future research directions. *Sensors*, *19*(1), 126.

[30]. Bennis, M., Debbah, M., & Poor, H. V. (2018). Ultrareliable and low-latency wireless communication: Tail, risk, and scale. *Proceedings of the IEEE*, *106*(10), 1834-1853.

[31]. Park, J., Samarakoon, S., Bennis, M., & Debbah, M. (2019). Wireless Network Intelligence at the Edge. *Proc. IEEE*, *107*(11), 2204-2239.